STRATEGY RESEARCH PROJECT

AN ANALYSIS OF CURRENT UNITED STATES HOMELAND DEFENSE POLICIES

BY

LIEUTENANT COLONEL KELLY L. MAYES
United States Army

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

AN ANALYSIS OF CURRENT UNITED STATES HOMELAND DEFENSE POLICIES

by

Lieutenant Colonel Kelly L. Mayes
U.S. Army

Colonel (Ret) Robert Coon
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Kelly L. Mayes

TITLE: AN ANALYSIS OF CURRENT UNITED STATES HOMELAND DEFENSE POLICIES

FORMAT: Strategy Research Project

DATE: 06 April 2000 PAGES :24 CLASSIFICATION: Unclassified

For the first time in many years the United States must re-consider its homeland defense policies. Gone are the days when deterrence was the only policy required. The emergence of the United States as the sole remaining world superpower has forced it to become more involved in international affairs. This involvement results in the alienation of other nations and non-state actors who are unable to directly challenge the United States and its policies.

Technological advances coupled with rapid globalization provide these potential enemies a myriad of capabilities to either directly attack the United States homeland or to use the threat of attack to shape its policies. Among the capabilities potential enemies may use are terrorism, ballistic missiles, cruise missiles, WMD, and cyber attacks. These capabilities are inexpensive, readily available; difficult to detect prior to an attack, and nearly impossible to assign responsibility for the attack once they are employed.

The United States currently has or is in the process of developing numerous policies and programs in an effort to counter these threats. But to date the result has been the creation of a myriad of laws, policies and programs that fail; to assign an overall lead agency; are fragmented; that fail to address all the potential threats. Critical to this development of a homeland defense policy for the United States is the determination of what roll the armed forces should play. Some officials want the armed forces to create a command charged with overall responsibility for homeland defense. But this idea dismays many senior military leaders who want to focus on war fighting and many civilians who are concerned that giving the mission to the armed forces might undermine the concept of civilian rule.

The end result is that currently the United States has no overarching policy to ensure the protection of its homeland and its citizens. Failure to develop a coherent, synchronized homeland defense policy will result, at best in the wasting of billions of dollars, and at worst in the loss of many lives.

In this paper we will look at the potential threats to the homeland of the United States; review current laws and polices designed to counter these threats; and the role the armed forces play in executing these policies. Following this will be a discussion on what is needed to develop a viable homeland defense policy and the role the military should play in that policy.

TABLE OF CONTENTS

AN ANALYSIS OF CURRENT UNITED STATES HOMELAND DEFENSE POLICIES

Now that an immediate peril is not plainly visible, there is a natural tendency to relax and to return to business as usual ... But I feel that we are seriously failing in our attitude toward the international problems whose solution will largely determine our future.

George C. Marshall[1]

For over two hundred years the United States has relied upon its geopolitical positioning to defend itself from enemies. Weaker, non threatening neighbors to the North and South coupled with vast oceans on the East and West have ensured that for most of its history the United States has been free from worrying about the defense of the homeland. Even the one enemy who could threaten to directly attack the homeland of the United States disappeared with the end of the Cold War and the subsequent collapse of the Soviet Union. But the United States can not become complacent. Rapid advances in technology and increasing globalization are beginning to mitigate the geopolitical advantage the United States has relied on for so long.

The emergence of the United States as the world's only super power has forced it to take a greater role in global politics, which in turn has caused the alienation of some countries and groups. These countries and groups do not have the capability to directly challenge the U.S. economically, militarily, or diplomatically so they must look to other means to accomplish their objectives. Unfortunately, for the United States the means these adversaries select may not fall into the traditional categories of national power and may maximize the use of technology to overcome the benefits of the U.S. geopolitical position. The bottom line is that the U.S. is in a position where it can no longer ignore the defense of its homeland and must develop a plan for the physical security of its territory and people.

Over the last several years there has been much debate at the highest levels of the United States government on how best to protect itself from these new threats, but efforts to date have been disjointed and fail to address the full spectrum of threats in a comprehensive strategy. The result is a dysfunctional approach that at its best wastes millions of dollars and at worst will result in the deaths of untold numbers of United States citizens.

Some policy makers argue that the responsibility for homeland defense should rest with the armed forces. These people advocate the creation of a new unified command, or assigning the mission to Joint Forces Command and by default, militarizing the issue. This approach, its proponents argue, ensures unity of effort, centralized control, and maximizes the large investment of tax dollars already spent. But is that the answer?

In this paper we are going to look at the issues associated with homeland defense for the United States. Specifically the paper will look at the threat, current homeland defense policies of the United States, and finally the role the U.S. military should play in homeland defense. The

intent of this paper is not to propose a solution to this complicated issue, but rather to provide a background for further discussion and thought.

THE THREAT

> The United States has entered a period that presents both opportunities and challenges. Our nation is at peace and much of the world embraces the democratic ideals we cherish. The threat of nuclear war has diminished and diplomatic efforts continue to reap benefits in creating a more stable and peaceful world. Nonetheless, there remain a number of uncertainties, including potentially serious threats to America's security. Principal among these are regional dangers, asymmetric challenges, transnational threats, and wild cards. This uncertain environment would be even more threatening without the American engagement and leadership that this strategy supports.[2]

In reality only one of the threats mentioned in the National Military Strategy cited above has the potential to directly impact the United States homeland and that is asymmetrical threats. Asymmetrical threats are those actions a potential enemy might take that are not of a conventional military nature. Due to the military superiority of the United States potential enemies, whether nations or non state actors, will be more likely in the future to resort to terrorist acts or unconventional attacks against vulnerable civilian targets and critical national infrastructure in the United States to achieve their aims. Modern advances in biotechnology and pharmaceutical manufacturing provide a growing number of nations and terrorist groups inexpensive highly destructive weapons with which they may attack U.S. society. Of special concern are threats of terrorism, the use or threatened use of weapons of mass destruction, (WMD), and information warfare.

TERRORISM

Military and intelligence experts believe that the greatest threat to the United States homeland is posed by terrorist groups that have no affiliation with another nation.[3] This threat is further compounded by the fact that various groups internal to the United States have shown a willingness to use terrorism to advance their goals. The real threat poised by non-state sponsored or domestic terrorists is the difficulty in deterring their attacks.

Nations that might contemplate attacking the United States homeland are deterred from doing so because of the disproportionate retaliation they would face. The military might of the United States coupled with precision guided munitions and its nuclear arsenal result in almost a certainty that attacks to the United States homeland by other nations or rouge states can be deterred. Conversely it is unlikely that the military forces of the United States could deter non-state actors (terrorists, criminals or others) who are seeking to coerce or punish the United States or its allies.

One of the major obstacles in deterring potential acts of terrorism today is the difficulty in attributing an attack to any particular group. Today's terrorist is less likely to brag about their actions and freelance groups either external or internal are difficult to trace. Today's terrorist

groups are highly decentralized, privately financed, and their members are extremely suspicious of outsiders. Infiltration of these groups by the intelligence apparatus of the United States is difficult because the groups are likely to have fanatical religious or ideological zeal holding it together. Usually these groups are based in failed states that have no or limited contact with the United States. These failed states provide a secure base for terrorist groups while the information revolution gives them global access.

Terrorist and religious cults have an obsession with the United States because of its superpower status and behavior. As the sole remaining superpower, the United States is called upon more and more frequently to respond to international crises and deploy forces around the world. This increased involvement in international affairs by the United States will ultimately alienate some nations and groups who will want to influence United States actions. The military strength of the United States will deny these disenfranchised states and groups the ability to engage in overt attacks against the United States and they will be driven to employ asymmetric means to influence United States policy.

The threat of terrorist attack against the United States homeland is real and will continue to increase as other nations and non-state actors look for ways to overcome the conventional military strengths of the United States. The military superiority of the United States cannot shield the country completely from attacks of terrorism, either external or internal. Additionally this threat is being facilitated by a proliferation of technologies associated with WMD (chemical, biological, and nuclear weapons).

WEAPONS OF MASS DESTRUCTION

> With advanced technology and a smaller world of porous borders, the ability to unleash mass sickness, death, and destruction today has reached a far greater order of magnitude. A lone madman or nest of fanatics with a bottle of chemicals, a batch of plague-inducing bacteria, or a crude nuclear bomb can threaten or kill tens of thousands of people in a single act of malevolence.[4]

The destruction described in the statement above is attributed to WMD. Increasingly the technology required to produce and deliver WMD to the homeland of the United States is becoming available to potential enemies. Further complicating the problem is the fact that the technologies required for producing these weapons have legitimate functions in society. The same knowledge and technology needed to develop chemical or biological weapons are also critical to such mainstream products as pesticides, vaccines, and a wide variety of manufactured goods.[5] This makes efforts by the United States to detect and deter their production nearly impossible. The question for the United States is not only when, but also how these attacks will occur. There are three primary ways in which an enemy of the United States could employ WMD; Ballistic Missile attack, Cruise Missile attack; and WMD delivered by other means.

Weapons of Mass Destruction Delivered by Ballistic Missiles

One of the ways a nation or non-state actor hostile to the United States might attack the homeland is with ballistic missiles. While this threat is currently unlikely it can not be overlooked since ballistic missiles can carry either conventional or WMD war heads. In 1997 Congress established the Rumsfeld commission to assess the nature and magnitude of existing and emerging ballistic missile threats to the United States. In July of 1998 the commission reported that current United States analyses and practices needed to be revised to reflect the reality of an environment in which there may be little or no warning. Additionally the commission found that the threat posed by emerging capabilities is broader, more mature and evolving more rapidly than the intelligence community has reported.[6] Currently more than 25 countries either possess or are developing nuclear, biological, or chemical weapons and more than 20 nations are developing ballistic missiles. China, while not openly hostile, is reportedly poised to test a new mobile intercontinental ballistic missile capable of reaching the western United States.[7] On the other hand several countries openly hostile to the United States are pursuing ballistic missile technology, (Libya, Iraq, Iran, Syria, and North Korea), but none currently have a missile that can reach the United States and according to United States intelligence estimates that capability is over a decade away.[8]

The threat of a ballistic missile attack of the United States is mitigated by the capability of the United States to detect their launches. Through the use of satellites equipped with infrared sensors the United States can detect the launch plume of a ballistic missile and determine the point of origin. This capability enables the United States to use the threat of retaliation to deter ballistic missile attacks by other nations.

This threat of retaliation by the United States would probably not deter non-state actors from launching a ballistic missile attack on the United States if they had the capability to do it. United States intelligence experts believe that the technical sophistication required to develop and launch a ballistic missile that could hit the United States is beyond the capabilities of non-state actors.

So while the United States must be concerned with an attack on the homeland by ballistic missiles it is probably the least of the threats it will face. More likely is an attack by a land attack Cruise Missile.

WMD Delivered by Cruise Missiles

Like ballistic missiles cruise missiles can carry either conventional or WMD warheads. The major advantages of cruise missiles are that they are less expensive and more accurate than ballistic missiles. The smaller size and ground hugging flight characteristics of cruise missiles make them more difficult to detect and engage.

Today short-range anti-ship cruise missiles are available in large quantities. And while it is true that only a few countries possess long range land attack cruise missiles there, are no technological barriers that would prevent a nation or non state actor from converting a short range missile into a long range missile. Cruise missiles can be launched from air, land, or sea, making detection of their launch point difficult and retaliation impossible. This factor, coupled with cheap costs and availability, makes cruise missiles not only attractive to terrorists groups but also to rogue nations.

WMD Delivered by other Means

Perhaps the most dangerous threat to the United States homeland is a WMD attack by a terrorist group using very simple delivery means. The openness of United States culture, combined with liberal immigration laws and large undefended borders, allows persons or groups wishing to do harm easy infiltration into the country. This kind of attack would be almost impossible to prevent and once executed finding the individuals responsible would be difficult at best.

The attack by the Japanese cult, Aum Shinrikyo, on 20 March1995 demonstrates the ease of delivering WMD. Using simple, commercially bought aerosol dispensers, the group was able to attack five separate targets simultaneously with the nerve agent sarin. While the attack failed to achieve the level of destruction sought by the cult, it did result in 12 deaths, 5,500 injuries and not only shook Japan but also the world.

As of June 1999, there were 475 incidents worldwide recorded in the Study on Chemical, Biological, radiological, and Nuclear Terrorism database at the Monterey Institute of International Studies. Of these, 261 were classified as having been perpetrated by groups or individuals with political or ideological motivations.[9] In the United States in 1998 there were three instances of alleged anthrax bombs, in 1999 the number grew to 100. Fortunately none of the threats were real but they show willingness on the part of alienated groups to use WMD or the threat of WMD delivered by simple means as a way to influence the actions of the United States.

CYBER Attacks

The potential for an enemy to attack the information infrastructure of the United States as a means of undermining its economy and deterring or disrupting its operations abroad is of increasing concern. Among the critical infrastructure that may be targeted are telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. Attacks to the infrastructure could take one of two forms: physical attacks to tangible property or attacks by electronic means (Cyber attacks). Of these two ways of attack to a potential enemy the most likely is a cyber attack.

Cyber attacks are difficult to detect, and finding the initiator of such an attack is difficult. Additionally, the cost associated with such an attack is minimal especially in comparison to the

damage it can inflict. Threats and actual attacks on the commercial and defense information infrastructure of the United States are on the rise. In a recent speech given to the Army War College at Carlisle Barracks Pa. General Meigs, Commanding General United States Forces Europe, said there were 2.5 million attacks on the computer network in his command last year.[10]

The reliance of the United States on global commercial telecommunications infrastructures to pursue its interests as the world's sole superpower further complicates the situation. The threat is further compounded by the fact that many of these critical infrastructures are privately owned.

COUNTERING THE THREAT

"We don't know when and we don't know the place, but we will be attacked."[11]

Protecting the territory of the United States and its citizens from "all enemies both foreign and domestic" is the principal task of the government. But as the proceeding section illustrates besides the need to deter a strategic nuclear attack, the United States must also defend itself against terrorism, ballistic and cruise missiles, WMD, and Cyber attacks.

The diversity of these potential threats makes planning for homeland defense complicated. The lines between domestic and foreign policy, intelligence and information, political and economic agendas and military and law enforcement activities become increasingly blurred. Many of the emerging challenges to the security of the United States respect no national boundaries and their perpetrators have no national affiliation.

In order to overcome these challenges the United States must develop a homeland defense strategy that is coordinated and executed among multiple layers of governmental agencies at the local, state, national, and international levels.

Towards this goal of developing an effective homeland defense strategy the United States has implemented several policies ranging from public laws to Presidential Decision Directives all geared towards not only countering the threat, but also toward synchronizing the efforts of the various local, state, national and international agencies involved. Unfortunately all have fallen short of the goal.

In this section we will look at key United States homeland defense policies in order to determine why they are inadequate. Additionally in this section we will look at the role the armed forces of the United States play in current homeland defense policies.

KEY UNITED STATES HOMELAND DEFENSE POLICY

> ...Due to our military superiority, potential enemies, whether nations or terrorist groups, may be more likely in the future to resort to terrorist acts or other attacks against vulnerable civilian targets in the United States instead of conventional military operations. ... The Federal Government will respond rapidly and decisively to any terrorist incident in the United States, working with state and local governments to restore order and deliver emergency assistance.[12]

During the Cold War, U.S. homeland defense planning was focused almost exclusively on the threat of a large, deliberate Soviet nuclear missile attack. The difficulties of successfully intercepting such an attack led policymakers to rely on deterrence rather than actual defenses to protect the United States homeland. But as already discussed, deterrence is not likely to have any effect on non state actors looking to hit the United States with terrorism, cruise missiles, WMD, or cyber attacks. In light of these new threats, United States policy makers have initiated several key policies and programs in an attempt to implement a viable defense.

PDD 39

In 1995 following the sarin gas attack in Japan and the Oklahoma City bombing, President Clinton signed Presidential Decision Directive (PDD) 39 "United States Policy on Counterterrorism". The PDD states that "The United States shall give the highest priority to developing capabilities to ...manage the consequences of nuclear, biological, or chemical material or weapons used by a terrorist."[13] PDD 39 further goes on to reinforce the interagency process for combating terrorism, by directing lead agency responsibilities and support requirements for response to both domestic and overseas terrorist incidents.

PDD 39 divides the threat at home and abroad into two distinct categories: crisis response and consequence management. Crisis response refers to instances where the perpetrators of an assault are discovered before an actual release. Domestic crisis response is the responsibility of the FBI; while the Department of State, through its Office of Counterterrorsm, is accountable for overseas incidents.

Consequence management, by contrast, describes ways and means to alleviate the short and long-term physical, socio-economic, and psychological effects of a chemical or biological attack. Consequence management focuses on re-establishing "those essential services and activities required to manage and mitigate problems resulting from disasters and catastrophes. Such services may include transportation, communications, public works, mass care, resources support, health and medical services, urban search and rescue, hazardous materials, food, and energy."[14]Consequence management requires the coordination of international, national, regional, and local assets to deal with the effects of such an attack. Responsibility for domestic consequence management rests with the Federal Emergency Management Agency (FEMA) and with the Department of State for overseas incidents.

PDD 39 recognizes the fact that the Department of Defense possesses significant assets that could be used in either crisis response or consequence management. The Department of Defense has designated the Secretary of the Army as the Executive Agent for managing DoD responses to requests from civil authorities for military assistance. The Secretary of the Army in turn manages his overall response to civil emergencies through the Army's Director of Military Support (DOMS).

While PDD 39 is a positive step towards creating a homeland defense policy for the United States it still falls far short. First among its problems is the command and control concept of a lead Federal agency. As outlined in PDD 39, the FBI is responsible during the period prior to an attack, but then responsibility is transferred to FEMA once the attack occurs. At best this delineation of responsibility is arbitrary and confusing: "In any domestic disaster, [consequence management] is the crisis."[15] This arrangement creates jurisdictional problems between the FBI, which seeks to control the immediate situation and protect criminal evidence, and FEMA, which endeavors to stabilize the situation, save lives, and initiate protective and containment protocols. The command and control arrangement in PDD 39 also complicates the participation by the Armed Forces. Military personnel find themselves in an environment where rules of engagement, responsibilities, and chain of command are fluid at best.

PDD 39 also fails to take into account the requirement for prior coordination. Assembling a combined Federal response force capable of addressing a range of contingencies on short notice is impossible. An effective response program must be pre-planned, organized, and trained. In order to accomplish this, FEMA, Justice, and DoD must fully integrate their operations.

Another problem with PDD 39 is that it fails to address the full spectrum of threats to the homeland of the United States. As discussed in the threat section of this paper those wishing to harm or influence the actions of the United States may also use cyber attacks, or ballistic and cruise missile attacks.

Executive Order 13010

In light of the threat from cyber attack President Clinton, in 1996, issued Executive Order 13010, "Critical Infrastructure Protection." This Executive Order established the President's Commission on Critical Infrastructure Protection. This Interagency group consists of two full time members for the Departments of the Treasury, Justice, Defense, Commerce, Transportation, and Energy, the Central Intelligence Agency, the Federal Emergency Management Agency, the Federal Bureau of Investigation, and the National Security Agency. The overwhelming challenges that this commission faces center on the fact that many of these critical infrastructures are privately owned and, the dangers they face are difficult to detect and profile.

As with PDD 39, the executive order fails to identify one single agency or person charged with overall responsibility for execution. This failure to appoint a single person with the responsibility of protecting the critical infrastructures of the United States leads to political in fighting and duplication of effort.

National Defense in the 21st Century

In December 1997 the National Defense Panel rendered a report entitled Transforming Defense, National Security in the 21st Century. In a section of this report entitled Homeland

Defense the panel recommended several actions to be taken by the Department of Defense in order to ensure a viable homeland defense strategy.[16]

1. Develop integrated active and passive defense measures against the use of WMD.
2. Develop and retain the option to deploy a missile defense system capable of defeating limited attacks.
3. Incorporate all levels of government into managing the consequences of a WMD-type attack.
4. Prepare reserve components to support consequence management activities.
5. Support the recommendations of the President's Commission on Critical Infrastructure Protection.
6. Use Department of Defense assets to advise and assist law enforcement in combating terrorist activities.

Unfortunately the panel never addressed the issue of command and control responsibilities of homeland defense as delineated in PDD 39 and Executive Order 13010. The panel did acknowledge that "the terrorist threat to the United States is a complex issue which, as it encroaches upon U.S. territory, transitions from a Defense and State activity to one managed primarily by the Department of Justice or local law enforcement agencies. To date the hand-off of responsibilities and sharing of intelligence on known and suspected terrorists has not been properly delineated and may, in some areas be dysfunctional." [17] Yet, despite this acknowledgement they failed to recommend a solution.

In the final analysis the National Defense Panel report fell short of providing a comprehensive homeland defense policy.

Nunn-Lugar-Domenici Legislation

In 1996 Congress passed Public Law 104-201 National Defense Authorization Act for Fiscal Year 1997 TITLE XIV The Defense Against Weapons of Mass Destruction Act.[18] More commonly known as the Nunn-Lugar-Domenici Act, this legislation is Congress's attempt at reducing the United States vulnerability to terrorism and WMD attacks.

By providing funds for training and equipping local US emergency workers to respond to WMD attacks, the Act attempts to mitigate the effects of a WMD attack. By providing additional funds and equipment to aid the U.S. customs service in preventing smuggled weapons and WMD materials from entering the United States, the Act attempts to stop the proliferation of WMD. And, lastly, by establishing a national coordinator for counter-proliferation strategy at the National Security Council level the Act attempts to synchronize the efforts of over 40 Federal agencies to defend the homeland.[19]

But even this Act fails to address the entire threat. Missing is any mention of National Missile Defense (NMD) or cyber attack.

National Missile Defense

Since 1994, President Clinton and the Republican-led Congress have initiated several programs and expended millions of dollars to develop policies and systems to protect the United States from a ballistic missile attack launched by a rouge state. Towards this goal the United States, between FY1994-FY2005, has committed 13.9 billion dollars to develop a 50-state missile defense system.[20]

In March, 1998 the Congress of the United States in response to a report issued by the Rumsfeld Commission passed Senate Bill S257, the National Missile Defense Act of 1999. Despite 10 years of effort and billions of dollars, the United States still does not have any defense against ballistic missile attack. To date no successful tests of the technologies being developed have been conducted. Further complicating this problem is the fact that the development of a NMD capability by the United States risks worsening relations with Russia. The 1972 ABM treaty limits the United States and Russia to one ABM site each and forbids research and development of further ABM systems. Development of a NMD capability by the United States at a time when Russia is in a precarious position in terms of internal stability might strengthen the hand of Russian nationalists who accuse the United States of pursuing policies designed to keep Russia from returning to a world power.

The Current Role of the Armed Forces in Homeland Defense

""homeland defense is the defense mission of the next century"

Deputy Defense Secretary John Hamre[21]

The Department of Defense (DoD) is currently involved in all aspects of homeland defense; terrorism, information warfare, ballistic missiles, cruise missiles, and WMD attacks. Of all of the Federal agencies involved in homeland defense, DoD is arguably the best candidate to lead homeland defense efforts. DoD receives the largest share of the national budget, has an organic capability to protect its service members from WMD, and possesses the force projection capability to rapidly move to a crisis location. These facts have led some policy makers to argue that the armed forces should take the lead in all aspects of homeland defense. While indorsed by some this recommendation dismays many senior military leaders who want to focus on war fighting and alarms some civilian leaders who fear it challenges civilian control over the military. In this section of the paper we will look at current DoD homeland defense policies and programs in order to get an understanding of them and assess their potential for protecting the homeland of the United States.

DoD's current homeland defense program is composed of three components, nonproliferation, protecting U.S. forces and citizens against terrorists and WMD attacks, and response to mitigate damage if an attack does occur.

Non proliferation of technologies associated with missile and WMD procurement and production is the primary national objective of the United States. Towards this goal DoD contributes to a coordinated national and international effort by supporting the Cooperative Threat Reduction Program; DoD/FBI counterproliferation program; export control activities; and DoD inspection, verification, and enforcement support for the treaties and arms control regimes.[22] In all of these programs DoD is either the lead or co-lead agency. These existing programs have been responsible for considerable success in controlling the spread of WMD technologies and materiel form the former Soviet Union but they have not been as effective in dealing with the rest of the world. In 1999 both India and Pakistan demonstrated a nuclear capability and as already mentioned as many as 25 other countries are actively pursuing ballistic missile technology. Further hobbling U.S. nonproliferation efforts is the fact that non-state actors are not influenced by the normal tools of states craft.

DoD realizes that proliferation prevention might fail and rouge states or non-state actors determined to obtain WMD technologies and delivery systems might succeed. Given this DoD has, as directed by Congress and the President, initiated several policies and programs designed to protect the United States and its citizens from attack.

DOD directive 5134.9 signed in June 1994 established the Ballistic Missile Defense Organization, (BMDO). BMDO's mission is the protection of the United States against a limited ballistic missile attack. To fulfill this mission BMDO focuses on three programs: Theater Missile Defense (TMD), National Missile Defense (NMD), and advanced ballistic missile defense technologies. BMDO's objective is to provide an architecture upon which integrates all of the Services' requirements and capabilities. This architecture includes improving early warning and dissemination, ensuring communications, interoperability, and upgrading command and control centers.

In 1998 the DoD established the Joint Task Force for Computer Network Defense. Originally the task force worked for the Defense Information Systems Agency but with a change to the Unified Command Plan of 1999 the task force was assigned to U.S. Space Command.[23]

When nonproliferation and active defense fail DoD might be called on to respond in a consequence management role to mitigate damages. The Department of Defense has designated the Secretary of the Army as the Executive Agent for managing DoD responses to consequence management. The Secretary of the Army in turn manages his overall response to civil emergencies through the Army's Director of Military Support (DOMS). Initially DOMS was concerned with responding to natural disasters and found itself ill prepared to add the additional mission of homeland defense. In light of this DoD in October 1999 tasked Joint Forces Command to be prepared to provide military assistance to civil authorities in the event of an attack or an accident involving WMD. This mission will be performed by Joint Task Force Civil Support which will work directly for the Assistant Secretary of Defense for Civil Support.[24] In

response to the Nunn-Lugar-Domenici Act of 1996 DoD has developed a program to provide training and technical assistance to federal, state, and local emergency management personnel. This program managed by the Chemical and Biological Defense Command (CBDCOM) is spending millions of dollars to train first responders in 10 of the nation's largest cities. In 1998 DoD established the Consequence Management Program Integration Office to oversee the activities of the National Guard and reserve in establishing ten Rapid Assessment and Initial Detection (RAID) elements.[25] These RAID teams are designed to respond within four hours of notification and work with federal, state and local authorities to assess conditions, detect contaminates and provide technical advice.

ACTIONS REQUIRED FOR A VIABLE DEFENSE

"No one can terrorize a whole nation, unless we are all his accomplices."

Edward R. Morrow[26]

Current United States policies and programs are not sufficient to defend its homeland from attack. First, it is hard if not impossible to keep rogue states and non-state actors from obtaining the technologies and materiel necessary to strike the homeland of the United States. Treaties, sanctions, and world opinion, the normal tools of diplomacy with other nation states, have little if any impact on Rogue states and non-nation state players. Secondly, by focusing on rapid response instead of proactive defense the United States seems to be willing to accept an attack. Defense should encompass both passive and active measures. Current United States homeland defense policies tend to focus on passive measures such as purchasing decontamination equipment, training of response personnel, or on expensive big end items designed to counter the least likely threat, NMD. In order to provide for the security of its homeland and its people the United States must rethink its current policies.

First the command and control relationships of the numerous federal agencies involved in homeland defense must be streamlined. As the discussion above has shown there is no one person or agency in charge. Responding to the asymmetric threats identified in this paper requires closer cooperation between the armed forces and other government agencies. Traditional barriers between internal and external security and intelligence gathering must be overcome. Lack of coordination between domestic and foreign responsibilities is a major vulnerability.

The United States must be able to identify and penetrate emerging rogue state and non-state organizations and monitor their activities and prevent when possible their obtaining WMD capabilities or hostile acts. The United States must allocate more resources for developing this type of intelligence capability.

All potential threats to the homeland of the United States must be addressed in one capstone plan. Currently the United States has no capstone plan. Different policies, programs and laws address individual elements of the threat but no one plan or program addresses all the threats. The result is no unity of effort, no one agency or person responsible, and in-fighting over scarce resources.

The United States must accelerate its development of a NMD capability. The proliferation of ballistic missile technologies and an increase in the number of rogue states or non-state actors desiring to influence the actions of the United States makes defense against this threat more pressing. Additional resources need to be applied towards resolving technological problems and the program must be expanded to include defense against cruise missiles. Keeping operational control of this program in DoD is the best solution.

A public information campaign designed to educate Americans about the asymmetric threats they face and how the government plans to manage these threats must be initiated. An important component in deterring potential enemies from initiating WMD attacks is by demonstrating that WMD attacks will not force the United States change its policies. Some argue that revealing the threat to the American people might play into the hands of those wishing to inflict harm by creating hysteria, but my not informing them will make it difficult to obtain the resources required for developing realisitic defenses.

DoDs current train the trainer programs are a good beginning but are not the final answer to domestic preparedness training. DoD must develop a program for sustainment training and develop an exercise program that incorporates all agencies, (local, state, and), involved.

DoD must streamline the existing channels used to coordinate requests for military assistance. DoD Directive 3025.15 designates the Department of the Army as the executive agent for crisis management planning and implementation with responsibility to task service components and commit assets. This directive contradicts CJCS Instruction 3214.01 and the JSCP which assigns similar responsibilities to Joint Forces Command. DoD must combine leadership for defense of the homeland under one command. Continuing to leave responsibility under two separate organizations, DOMS and JFCOM, will only continue to confuse responsibilities and waste resources.

The United States must develop an information security program that strengthens the protection of critical infrastructure while denying access to those wishing to disrupt it. This security program must be built on international consensus and must share information on threats and vulnerabilities across local, state, federal, and international levels.

CONCLUSION

For the first time in many years the United States faces the reality of the threat of attack on its homeland and its people. The rapid expansion of technology coupled with globalization

and the emergence of the United States as the sole remaining super power has given rise to new potential enemies while giving them the means to attack the United States.

The United States, in an effort to protect itself form these threats, has enacted numerous laws, programs and executive orders all designed to create a viable homeland defense. To date these efforts, while a step in the right direction, have all fallen short and resulted in duplication of effort, competition for scarce resources and infighting. In order to develop a viable homeland defense United States policy makers must institute changes to current policies and programs. Among these are the need to clearly articulate what is meant by Military support to Civil authorities, streamlining current inter agency relationships, development of a more robust intelligence capability, acceleration of the NMD program, and the development of a comprehensive information security program. DoD currently plays a large roll in all of these missions and that is appropriate. What is missing from DoD is the assignment of a single command to take the lead. Spliting responsibility between DOMS, JFCOM, and Space command not only violates the principle of unity of command it also guarantees failure.

Word Count 6,114

ENDNOTES

[1] Washington's Birthday Remarks at Princeton University, 22 February 1947, quoted in Forrest C. Pogue, *George C. Marshall: Statesman* (New York: Viking Penguin, 1987).

[2] John M. Shalikashvili, National Military Strategy of the United States of America (Washington, D.C.: the Pentagon, 1997),1

[3] Ivan Eland, "Protecting the Homeland The Best Defense Is to Give No Offense," 5 May 1998; available from http://www.; Internet; accessed 6 February 2000.

[4] Ibid.

[5] Francis H. Marlo, "WMD Terrorism and US Intelligence Collection," Terrorism and Political Violence, vol. 11, no.3, (Autumn 1999): 53

[6] strategic assessment 1999 page 224

[7] Frank Nelson, "United States has No Missile Defense," January 25,1999; available from http://www.ncfd.org/pubs980125.html; Internet; accessed 26 February 2000.

[8] Ibid

[9] Gavin Cameron, "Multi-track Microproliferation: Lessons from Aum Shirikyo and Al Qaida," Studies in Conflict & Terrorism, vol.22, no.4, (1999): 277

[10]

[11] Paul Stone, "Guard, Reserve To Take on New Role," ; available from http://www.cadsim2.gmu.edu/mon/; Internet; accessed 15 December 1999.

[12] William J. Clinton, A National Security Strategy for a New Century, (Washington, D.C.: U.S. Government Printing Office, October 1998), 19.

[13] William J. Cohen, PROLIFERATION: THREAT AND RESPONSE (Washington D.C.: The Pentagon, 1997)

[14] John P. White, Department of Defense Directive 3025.15: Military Assistance to Civil Authorities, (Washington D.C.: Office of the Secretary of Defense, 1997), 1.

[15] Chris Seiple, "Consequence Management: Domestic Response to Weapons of Mass Destruction," Parameters, vol.27, no.3 (Autumn 1997), pp. 119-34.

[16] Philip A. Odeen, Transforming Defense-National Security in the 21st Century (Washington, D.C.: National Defense Panel, 1997), 25-28

[17] Ibid., 27.

[18] Zachary Seldon, "Nunn-Lugar: New Solutions for Today's Nuclear Threats," available from <http://www.bens.org/pubs/nunnlugar.html>; Internet; accessed 6 March 2000.

[19] Scott R. Taylor et al, "Consequence Management In Need of a Time Out" Joint Forces Quarterly 22 (Summer 1999): 78-79

[20] Rachel Dubin, "National Missile Defense and the Anti-Ballistic Missile Treaty: Risks and Strategies," available from <http://www.cdi.org.weekly/1999/issue13.html>; Internet; accessed 7 March 2000.

[21] Johnathan S. Landay, "Launching a 'homeland' defense," 29 February 1999; available fromhttp://www.csmonitor.com/durable/1999/01/29/fp1s1-csm.shtml: Internet; accessed 15 December 1999

[22]William J. Cohen, PROLIFERATION: THREAT AND RESPONSE (Washington D.C.: The Pentagon, 1997) 54

[23] Jim Garamone, "Unified Command Plan Changes Announced," 12 October 1999; available from http://ustcweb.safb.af.mil/news/991008-1.html; Internet; accessed 26 February 2000.

[24] JFCOM Brief

[25] Guard ReserveTake on New Role

[26] "Cartoons of the Century," Newsweek 134 (Dec. 20 1999): 64.

BIBLIOGRAPHY

Blechman, Barry M et al. The American Military in the 21st Century. New York: St. Martin's Press, 1993.

Cameron, Gavin, "Multi-track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida," Studies in Conflict & Terrorism, vol. 22, no. 4, (October-December 1999): 277

Carter, Ashton B. "Adapting Defense to Future Needs," Survival The IISSQuarterly, (Winter 1999-2000):101

"Cartoons of the Century." Newsweek 134 (Dec. 20 1999): 55-83

Clinton, William, Executive Order 13010: Critical Infrastructure Protection. Washington D.C.: The White House, 1996.

Drell, Sidney D.; Sofaer, Abraham D.; Wilson, George D., "The Present Threat," Hoover Digest, no.1 (2000): 110

Garamone, Jim. "Unified Command Plan Changes Announced." 12 October 1999. Available from http://ustcweb.safb.af.mil/news/991008-1.html. Internet. Accessed 26 February 2000.

Marlo, Francis H. "WMD Terrorism and U.S. Intelligence Collection" Terrorism and Political Violence, vol. 11, no.3, (Autumn1999): 53

McRae, Hamish. The World in 2020. Boston: Harvard Business School Press, 1994

Pike, John. "Enhance Domestic Terrorism Response (Nunn-Lugar-Domenici and Related Programs.)" Available from http://www.fas.org/pub/gen/mswg/msbb98/tt05wmd.htm. Internet; accessed 6 March 2000.

Seldon, Zachary. "Nunn-Lugar: New Solutions for Today's Nuclear Threats." Available from http://www.bens.org/pubs/nunnlugar.html. Internet. Accessed 6 March 2000

Snow, Donald M. The Shape of the Future The Post-Cold War World. Armonk, New York, London, England: M.E. Sharpe Inc.,1991

Taylor, Scott R. et al. "Consequence Management In Need of a Time Out," Joint Forces Quarterly 22 (Summer 199): 78-85

Welch, Claude E. Jr., and Arthur K. Smith. Military Role and Rule. North Scituate, Massachusetts: Duxbury Press, 1974

White, John P. Department of Defense Directive 3025.15: Military Assistance to Civil Authorities. Washington D.C.: Office of the Secretary of Defense, 1997.